UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

DEREK HEFLEY, individually and on behalf of all others similarly situated, Plaintiff, -v- **JOHNSON CONTROLS INC.,** Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

1. Plaintiff Derek Hefley ("Plaintiff") brings this Class Action Complaint ("Complaint") on behalf of Plaintiff and all others similarly situated against Defendant Johnson Controls Inc. ("Defendant") for failure to properly secure and safeguard Plaintiff's and Class members' personally identifiable information ("PII") stored within Defendant's information network and alleges as follows based upon information and belief, and the investigation of counsel, except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge.

NATURE OF THE CASE

2. Entities that handle sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—especially hackers with nefarious intentions — will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

3. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity

theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

4. Defendant knowingly obtains sensitive employee and business associate PII and has a resulting duty to securely maintain such information in confidence.

5. As discussed in more detail below, Defendant breached its duty to protect the sensitive PII entrusted to it.

6. As such, Plaintiff brings this Class action on behalf of himself and all other individuals whose PII was accessed and taken by unauthorized third parties during a data breach of the Defendant's system from February 1, 2023 through September 30, 2023, which was announced when Defendant began providing notices on or about July 4, 2025 ("Data Breach").

7. Upon information ana belief, the Data Breach impacted millions of individuals, and involved unauthorized access to internal business systems, including a file repository.

8. The data exposed in the Data Breach included "personal information provided to Defendant during the course of employment, contract work, while applying for a job, or through other interactions with Johnson Controls and its affiliates or subsidiaries," as Defendant reported.[1]

9. As a direct and proximate result of Defendant's inadequate data security, and its breach of its duty to handle PII with reasonable care, Plaintiff's PII was taken by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

10. Plaintiff is now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of his privacy, and similar

[1] *See* https://faq.jci.com/english-us (last accessed July 15, 2025).

forms of criminal mischief, and such risk may last for the rest of Plaintiff's life. Consequently, Plaintiff must devote substantially more time, money, and energy to protect himself, to the extent possible, from these crimes.

11. Plaintiff, on behalf of himself and others similarly situated, brings claims for negligence, negligence *per se*, breach of fiduciary duty, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

12. To recover from Defendant for their sustained, ongoing, and future harms, Plaintiff and Class members seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendant; 3) provide, at Defendant's own expense, all impacted victims with lifetime identity theft protection services; 4) disclose whether a ransom was paid to the hackers and if so, the amount thereof.

PARTIES

13. Plaintiff Derek Hefley ("Hefley") is an adult individual and, at all relevant times herein, has been a resident and citizen of Oklahoma City, Oklahoma, where he intends to remain.

14. Defendant Johnson Controls Inc. ("JCI") is a leader in engineering, manufacturing and servicing of building products and systems, including commercial HVAC equipment, industrial refrigeration systems, controls, security systems, fire detection systems and fire-suppression solutions. Entities under the JCI corporate umbrella include Tyco or Sensormatic Solutions.[2]

[2] *See* https://faq.jci.com/english-us (last accessed July 15, 2025).

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are over 100 members of the putative Class. Putative Class members include citizens of states other than Wisconsin, including Plaintiff, who is a citizen of the State of Oklahoma.

16. This Court has personal jurisdiction over Defendant as it has substantial contacts with this District, transacts business in this District, and is headquartered in Milwaukee, Wisconsin, which is in this District.

17. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is deemed to reside in this District because it is subject to the Court's personal jurisdiction with respect to this action and because a substantial part of the events giving rise to the claims asserted herein occurred in this District, and Defendant regularly conducts business in this District.

FACTUAL BACKGROUND

A. Defendant and the Services it Provides

18. Defendant receives and handles PII, including personal information provided to Defendant during the course of employment, contract work, while applying for a job, or through other interactions with JCI and its affiliates or subsidiaries.

19. Plaintiff was a JCI employee from 2006 through 2009 and entrusted his information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. By obtaining, collecting, and storing Plaintiff's PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's PII from unauthorized disclosure.

21. Upon information and belief, Defendant funds its data security measures from general revenue, including payments made by or on behalf of Plaintiff and the Class members, and revenue generated by the labor and services of Defendant's employees and former employees, including Plaintiff.

B. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm

22. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

23. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private information.

24. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

25. For example, in 2024, the number of data compromises in the United States stood at 3,158 cases, affecting over 1.35 billion individuals.[3]

26. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's current and former employees and business associates especially vulnerable to identity theft, tax fraud, medical fraud, credit, and bank fraud, and more.

[3] *See* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last accessed June 20, 2025).

27. PII is a valuable property right[4] and its value is measurable. American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[5] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

28. As a result of their real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

29. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[6]

30. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these

---

[4] *See* https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible") (last accessed July 15, 2025).
[5] *See* https://www.iab.com/news/2018-state-of-data-report/ (last accessed July 15, 2025).
[6] *See* United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last accessed July 15, 2025).

forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

31. Based on the value of its employees' and business associates' PII to cybercriminals and cybercriminals' propensity to target businesses, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendant Breached its Duty to Protect its Current and Former Employees' and Business Associates' PII.

32. JCI first became aware of, and responded to, the Data Breach on September 24, 2023, and disclosed the Data Breach in SEC filings on September 27, 2023, November 13, 2023, and December 14, 2023.[7]

33. Plaintiff received in the mail a notice dated July 4, 2025, a copy of which is attached hereto as **Exhibit 1**.

34. The Notice states:

> Given the nature and complexity of the data involved, Johnson Controls has been working diligently with a dedicated review team including internal and external experts to conduct a detailed analysis of the data that was taken from Johnson Controls' network. Based on this data analysis, we believe that the unauthorized actor took information about you including your name and date of birth, address, phone number, Social Security number, national identification number, employee identification number, employment benefits and compensation information, information related to employment or work for Johnson Controls, performance evaluation information, demographic information, and trade union or works council membership information.

[7] *See* https://otp.tools.investis.com/clients/us/johnson_controls1/SEC/sec-show.aspx?Type=html&FilingId=16953602&CIK=0000833444&Index=10000; https://otp.tools.investis.com/clients/us/johnson_controls1/SEC/sec-show.aspx?Type=html&FilingId=17052232&Cik=0000833444; and https://otp.tools.investis.com/clients/us/johnson_controls1/SEC/sec-show.aspx?Type=html&FilingId=17119904&CIK=0000833444&Index=10000 (last accessed July 15, 2025).

See Exhibit 1.

35. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures to protect its current and former employees' and business associates' PII.

36. The injury from the Data Breach is worsened due to Defendant's extremely belated disclosure – occurring *years* after the Data Breach.

D. FTC Guidelines Prohibit Defendant from Engaging in Unfair or Deceptive Acts or Practices

37. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

38. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

39. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[8]

40. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords

[8] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed July 15, 2025).

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[9]

41. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

42. Defendant failed to properly implement basic data security practices.

43. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

44. Defendant was at all times fully aware of its obligations to protect current and former employees' and business associates' PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Individuals at an Increased Risk of Fraud and Identity Theft

45. Cyberattacks and data breaches at companies that store PII are especially problematic because they can negatively impact on the overall daily lives of individuals affected by the attack.

[9] *Id*.

46. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

47. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

48. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

49. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone

[10] *See* https://www.gao.gov/products/gao-07-737 (last accessed June 20, 2025).

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[11]

50. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Personal information is valuable to identity thieves, and if they can get access to it, they will use it to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

51. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

52. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.

53. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of data breach victims themselves.

54. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of

[11] *See* https://www.identitytheft.gov/Steps (last accessed June 20, 2025).

identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff.

55. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

56. Social Security numbers are particularly sensitive pieces of personal information. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits. Identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may be undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

57. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as the credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.

58. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Defendant is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market.

59. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notified the individual's employer of the suspected fraud.

60. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

61. It is within this context that Plaintiff must now live with the knowledge that Plaintiff's PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

62. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on Plaintiff's everyday life, including purchasing identity theft and credit monitoring services every year for the rest of Plaintiff's life, placing "freezes" and "alerts" with credit reporting agencies, contacting his financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

63. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiff's PII.

64. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to Defendant is removed from Defendant's files.

F. Plaintiff and the Class Suffered Damages

Facts Relevant to Plaintiff

65. Plaintiff is a former employee of Defendant.

66. Plaintiff was employed at JCI from 2006 through 2009.

67. As a condition of his employment with Defendant, he was required to provide his PII to Defendant.

68. Defendant retained Plaintiff's PII in its systems at the time of the Data Breach.

69. Plaintiff received the Notice, as detailed *supra* and annexed as Exhibit 1.

70. As a result, Plaintiff was injured by Defendant's Data Breach.

71. In requesting and maintaining Plaintiff's PII for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class members' PII. Defendant did not, however, take proper care of Plaintiff's and Class members' PII, leading to their exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

72. Moreover, Defendant failed to notify Plaintiff of the impact to his data – and indeed, failed to timely provide notice to the putative Class – until years after the Data Breach.

73. Upon receiving the Notice, Plaintiff spent time reviewing his credit reports, reviewing various credit alerts received by text and email, checking his financial information, and dealing with increased spam text messages and emails.

74. Plaintiff suffered a theft of thousands of dollars from his bank account in March of 2025 which, upon information and belief, was accessed by use of his PII, which may include password and login information and other data relevant for a hacker to access his bank account and steal thousands of dollars, including his and payroll or banking information. Plaintiff has also begun to receive scam texts and emails on a regular basis since the Data Breach occurred.

75. Plaintiff has also suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

76. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy. The risk is not hypothetical, as cybercriminals intentionally stole the data, misused it, threatened to publish, or have published it on the Dark Web, and the sensitive information, including names and Social Security numbers, which is the type of PII used to perpetrate identity theft or fraud.

77. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant, which was compromised in and because of the Data Breach.

78. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

79. Plaintiff has a continuing interest in ensuring that his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff's And Class Members' Damages

80. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways. Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

81. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's misconduct.

82. As a result of Defendant's failures, Plaintiff and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

83. Plaintiff is also at a continued risk because Plaintiff's information remains in Defendant's computer systems, which have already been shown to be susceptible to compromise and attack and are subject to further attacks so long as Defendant fails to undertake the necessary

and appropriate security and training measures to protect employees', former employees', and business associates' PII.

84. In addition, Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their PII to strangers.

CLASS ALLEGATIONS

85. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as: **All individuals residing in the United States whose PII was compromised in the Data Breach affecting Defendant in September 2023, including all those individuals who received notice of the Data Breach** ("Class").

86. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

87. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when he moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

88. **Numerosity** – Fed. R. Civ. P. 23(a)(1): Plaintiff is informed and believes, and thereon alleges, that there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

89. **Commonality** – Fed. R. Civ. P. 23(a)(2): This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendant has a duty to protect Plaintiff's and Class members' PII;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class members' PII, and breached its duties thereby;

c. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

d. Whether Defendant breached its duty of confidence to Plaintiff and the Class;

e. Whether Defendant violated its own Privacy Practices;

f. Whether Defendant entered a contract implied in fact with Plaintiff and the Class;

g. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and Class members' PII;

h. Whether Defendant was unjustly enriched;

i. Whether Plaintiff and Class members are entitled to damages as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct.

90. **Typicality** – Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in Defendant's system(s), each having their PII exposed and/or accessed by an unauthorized third party.

91. **Adequacy of Representation** – Fed. R. Civ. P. 23(a)(3): Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

92. **Injunctive Relief** – Fed. R. Civ. P. 23(b)(2): Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

93. **Superiority** – Fed. R. Civ. P. 23(b)(3): A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

94. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

95. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard employees', former employees' and business associates' PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

96. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the Data Breach.

FIRST CAUSE OF ACTION
NEGLIGENCE

97. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

98. Plaintiff brings this claim individually and on behalf of the Class.

99. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

100. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

101. Defendant has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

102. Defendant breached the duties owed to Plaintiff and Class members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class members' PII, Defendant breached its duties through the following errors and omissions that allowed the Data Breach to occur:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee and business associate information that resulted in the unauthorized access and compromise of PII;

b. failing to timely notify affected Class members;

c. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

d. failing to design and implement information safeguards to control these risks;

e. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

f. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

g. failing to detect the breach at the time it began or within a reasonable time thereafter;

h. failing to follow its own privacy policies and; and

i. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

103. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

104. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent

charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant' possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data;

i. Unauthorized bank account access and theft of funds;

j. Phishing email and text scams; and

k. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

105. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*

106. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

107. Plaintiff brings this claim individually and on behalf of the Class.

108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant' duty to protect Plaintiff's and the Class members' sensitive PII.

109. Defendant breached its duties to Plaintiff and Class members under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its employees, former employees and business associates.

110. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

111. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

112. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

113. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

114. Plaintiff brings this claim individually and on behalf of the Class.

115. Plaintiff and Class members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

116. As a recipient of employees', former employees', and business associates' PII, Defendant has a fiduciary relationship to Plaintiff and the Class members.

117. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

118. Defendant owed a fiduciary duty under common law to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

119. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class members' records.

120. Defendant had possession and knowledge of confidential PII of Plaintiff and Class members, information not generally known.

121. Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

122. Defendant breached its fiduciary duties owed to Plaintiff and Class members by, among other things: mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of PII; mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; failing to design and implement information safeguards to control these risks; failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; failing to evaluate and adjust its information security program in light of the circumstances alleged herein; failing to detect the breach at the time it began or within a reasonable time thereafter; failing to follow its own privacy policies and practices; and failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

123. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class members, their PII would not have been compromised.

124. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

125. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT

126. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

127. Plaintiff brings this claim individually and on behalf of the Class.

128. Upon information and belief, Defendant funds its data security measures entirely from general revenue, including payments made by or on behalf of Plaintiff and the Class members to Defendant, and from revenue generated by their labor and employment services for members of the Class that are employees or former employees.

129. As such, a portion of the payments made by or on behalf of Plaintiff sand the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

130. Plaintiff and Class members conferred a benefit on Defendant by their employment and/or otherwise performing work for Defendant.

131. In exchange, Plaintiff and Class members should receive from Defendant the consideration of adequate protection in the subject of the transaction of their employment and consumption and have their PII/PHI protected with adequate data security.

132. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class members for business purposes.

133. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize profits over security.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by common law and statutory duties.

135. Defendant failed to secure Plaintiff and Class members' PII and, therefore, did not provide full consideration for the benefit Plaintiff and Class members provided.

136. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

137. If Plaintiff and Class members knew that Defendant had not reasonably secured their PII, they would not have agreed to have their information provided to Defendant.

138. Plaintiff and Class members have no adequate remedy at law.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to

commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

140. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

141. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them in their employment with Defendant and/or consumption of Defendant's products and services.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT

142. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

143. Plaintiff brings this claim individually and on behalf of the Class.

144. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

145. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII. Plaintiff and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

146. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employees' PII.

147. Defendant still possesses Plaintiff's and Class members' PII.

148. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class members' PII in a manner that details that the measures have adequately addressed the underlying weakness in Defendant's systems targeted by the criminal hackers in the Data Breach.

149. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

150. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Defendant's networks. The risk of another such breach is real, immediate, and substantial.

151. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs in Defendant's systems, Plaintiff and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

152. Issuance of the requested injunction will not compromise the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach in

Defendant's systems, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other employees whose PII would be further compromised.

153. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment ordering Defendant to implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, demands relief as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer and employee data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant' wrongful conduct;

e) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all claims so triable.

July 16, 2025

/s/ Electronically signed by Patrick J. Schott

Patrick J. Schott
State Bar ID #: 1001913
SCHOTT BUBLITZ & ENGEL S.C.
640 W. Moreland Blvd.
Waukesha, Wisconsin 53188
Telephone: (262) 827-8920
pschott@sbe-law.com

Rachele R. Byrd (*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER
FREEMAN & HERTZ LLP
750 B Street, Suite 1820,
San Diego, CA 92101
Telephone: 619-239-4599
byrd@whafh.com

James F. Woods (*pro hac vice forthcoming*)
Annie E. Causey (*pro hac vice forthcoming*)
WOODS LONERGAN PLLC
One Grand Central Place
60 East 42nd St., Suite 1410
New York, NY 10165
Telephone: 212-684-2500
jwoods@woodslaw.com
acausey@woodslaw.com

Jon Tostrud (*pro hac vice forthcoming*)
Anthony Carter (*pro hac vice forthcoming*)
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310-278-2600
Facsimile: 310-278-2640
jtostrud@tostrudlaw.com
acarter@tostrudlaw.com

Attorneys for Plaintiff